C. **REMARKS**

Status of the Claims

Claims 1-20 are currently present in the Application, and claims 1, 8, and 14 are independent claims. Claims 1, 3, 5, 6, 8, 10, 12, 13, 14, 16, 18, and 19 have been amended, claims 2, 9, and 15 have been cancelled, and no claims have been added.

Examiner Interview

Applicants note with appreciation the telephonic interview conducted between Applicants' representative, Examiner Khoshnoodi, and Primary Examiner Lamarre on July 25, 2005. During the telephonic interview, the Examiner, the Primary Examiner, and Applicants' representative discussed the 102 reference (Win, et al., U.S. Patent No. 6,182,142). In particular, Applicants' representative discussed that Applicants' invention includes a strikeout server that receives, from multiple computer systems, failed login attempts and adds together the total number of failed login attempts from all the computer systems corresponding to a particular user. If the total number of failed login attempts exceeds a pre-defined number, the strikeout server revokes the user's password. In contrast, Win never discloses tracking failed login attempts from a plurality of computer systems, but rather uses an access server as a single login point and, once the user is authenticated, the user may access multiple protected servers based upon the user's roles.

The Examiner, the Primary Examiner, and Applicants' representative discussed amending the independent claims to more distinctly claim receiving failed login attempt messages from a plurality of servers. The Examiner noted that the amendment

should specifically read over column 27, lines 7-27 in Win. Applicants have made such amendments in this response.

IN addition, Applicants' discussed that Applicants received an objection to the oath/declaration because the Office Action suggests that it did not have all of the inventor's signatures. The Primary Examiner reviewed the oath/declaration and stated that the oath/declaration did in fact have all of the inventor's signatures and, therefore, the objection was overcome.

Oath/Declaration

The oath or declaration stands incompliant to 37 CFR 1.67(a) because the office action suggests it was not signed by all the inventors. As discussed above, all of the inventors did sign the oath/declaration and, therefore, Applicants request removal of the objection to the oath/declaration.

Claim Rejections - Alleged Anticipation Under 35 U.S.C. § 102

Claims 1-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Win et al. (U.S. Patent No. 6,182,142, hereinafter "Win"). Applicants respectfully traverse these rejections.

As discussed with the Examiner and the Primary Examiner, Applicants have amended the independent claims to distinctly claim receiving messages from a plurality of computer systems, which was claimed in Applicants' original claim 2. Applicants' independent claims as amended are directed to "managing invalid password attempts" with limitations including:

- receiving a message corresponding to a failed login attempt from one of a plurality of computer systems that receives user login requests, wherein the message includes a distinguished name;

- calculating a total failed login attempt number corresponding to the distinguished name, the total failed login attempt number including the summation of failed login attempts corresponding to the distinguished name that are received from the plurality of computer systems;
- identifying a failed login attempt allowed number;
- determining whether the total failed login attempt number is greater than the failed login attempt allowed number; and
- revoking a password corresponding to the distinguished name based upon determining that the total failed login attempt number is greater than the failed login attempt allowed number;

Applicants' invention receives failed login attempts from a plurality of computer systems and calculates the total number of failed login attempts for each distinguished name. For example, computer system A may send two failed login attempt messages for a particular distinguished name, and computer system B may send three failed login attempt messages for the same distinguished name. In this example, Applicants' invention adds the failed login attempts together, resulting in five total failed login attempts. Applicants' invention then compares the total failed login attempt quantity with a failed login attempt allowed number to determine whether to revoke the corresponding user's password.

In contrast, Win never teaches or suggests receiving failed login attempts from a plurality of servers, but rather discloses a single server (access server) as a single login point. Once logged in, a user is able to communicate with multiple protected servers. Win states:

> "Using a method for controlling access to information resources, a single secure sign-

> on gives the user access to authorized resources, based on the user's role in the organization." (Abstract)

This is opposite of Applicants' invention, in that Applicants invention provides multiple sign-on servers, and Applicants' strikeout server tracks the summation of failed login attempts at all of the sign-on servers. Win continues to disclose that an access server provides a single universal point of access:

> "FIG. 5A is a state diagram of steps carried out by Access Server 106 in a preferred embodiment. As shown by state 502, browser 100 opens the URL of a login page. The login page prompts the user for a name and password, as shown in state 504. Preferably, a single login page is provided, regardless of the number of Web applications to which the user has access. Thus, the system 2 provides single secure login to Intranet or Extranet Web applications. The login page provides a single universal point of access to authorized applications and content." (col. 9, lines 53-62, emphasis added)

Win does disclose the use of multiple access servers in a mirrored environment, but each one of these access servers functions independently of the other access servers, and, therefore, Win never discloses tracking the summation of failed login attempts at all of the access servers as claimed by Applicants. In fact, Win discloses details of the access server and how a "login tracking service" that is located within each access server internally tracks failed login attempts at an access server. Win states:

> "For each login attempt, the Login Tracking Service logs the user's login activity. It saves the time of last successful and

> unsuccessful logins and number of consecutive, unsuccessful login attempts." (col. 10, lines 6-9)

The login tracking service is located within authentication client 414 shown in Win's Figure 4 (col. 9, lines 34-36). As can be seen by viewing Win's Figure 4 and corresponding text, the login tracking service never receives external failed login attempts from other access servers. In fact, when Win uses multiple access servers, each of the access servers has its own login tracking service and, therefore, Win never discloses tracking the total amount of failed login attempts for a user at all the access servers as claimed by Applicants.

Win's col. 27, lines 7-27 were referenced during the Examiner Interview in an effort to point out that Win discloses receiving failed login attempt messages from a plurality of computer systems. However, after further review, this reference never discusses receiving failed login attempts, but rather discloses how a computer system that implements Win's invention is able to remotely receive computer readable medium (e.g. a program that implements the invention). Specifically, Win states:

> "Fig. 9 is a block diagram that illustrates a computer system 900 upon which an embodiment of the invention may be implemented... According to one embedment of the invention, controlling access to protected information resources is provided by computer system 900 in response to processor 904 executing one or more sequences of one or more instructions contained in main memory 906. Such instructions may be read into main memory 906 from another computer-readable medium...Various forms of computer readable medium may be involved in carrying one or

> more sequences of one or more instructions to processor 904 for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem... a modem local to computer system 900 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal [that is converted and stored in main memory.]" (col. 26, line 2 - col. 27, line 16, emphasis added)

As can be seen, the above reference discloses receiving program instruction sequences that execute Win's invention, but never discloses receiving failed login attempts, let alone receiving failed login attempts from a plurality of computer systems as claimed by Applicants.

To continue with the reference discussed during the Examiner Interview, Win discloses that the computer system capable of implementing Win's invention includes a standard network communication interface:

> "Computer system 900 also includes a communication interface 918 coupled to bus 902. Communication interface 918 provides a two-way data communication coupling to a network link 920 that is connected to local network 922..." (col. 27, lines 17-21, emphasis added)

As can be seen, the above reference discloses communicating over a network, but never discloses receiving failed login attempts, let alone receiving failed login attempts from a plurality of computer systems as claimed by Applicants. In fact, as discussed above, Win never teaches or suggests collecting failed login attempts from a plurality of access

servers because each access server tracks its own failed login attempts with its internal login tracking service.

The Office Action uses two references in Win to reject Applicants' original claim 2 limitation of receiving a message from a plurality of computer systems. However, after further review, the two references never disclose receiving messages from a plurality of computer systems as claimed by Applicants. The first references states:

> "The foregoing components cooperate to control access to resources stored on one or more protected servers 104, 112" (col. 4, lines 44-46)

The above reference discloses multiple protected servers. The protected servers, however, are not the servers that Win uses for login authorization. The protected servers include data that a user accesses once the user has logged in using Win's access server. The above reference never teaches or suggests using multiple access servers, let alone tracking the total amount of failed login attempts at a plurality of computer systems as claimed by Applicants.

The Office Action's second reference to reject Applicants' original claim 2 states:

> "In the preferred embodiment, Administration Application 114 displays a server administration screen. An administrator enters, for each protected server 104, an identifier, a name, a protocol, a port, a description, the location of an authentication server, URLs that identify pages displayed upon logout, upon login, and where restricted resources are encountered..." (col. 7, lines 56-62)

Again, the above reference discloses multiple protected servers. As discussed above, the protected servers are not the servers for authorizing the user and, therefore, the protected servers never track failed login attempts. As can be seen from the above discussion, Win never teaches or suggests "calculating a total failed login attempt number...the total failed login attempt number including the summation of failed login attempts ... that are received from the plurality of computer systems" as claimed by Applicants. In addition, Win never teaches or suggests Applicants' determining and/or revoking limitations included in Applicants' claim 1. Therefore, since Win never teaches or suggests all the limitations included in Applicants' claim 1 as amended, amended claim 1 is allowable over Win.

Claim 8 as amended is an information handling claim including similar limitations to amended claim 1 and, therefore, is allowable for at least the same reason as amended claim 1. Claim 14 is a computer program product claim including similar limitations to amended claim 1 and, therefore, is allowable for at least the same reason as amended claim 1.

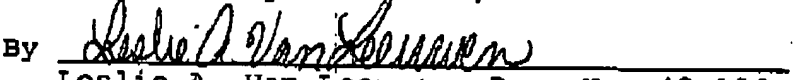
Each of the remaining claims 3-7, 10-13, and 16-20 each depend, directly or indirectly, on one of the allowable independent claims 1, 8, and 14. Therefore, claims 3-7, 10-13, and 16-20 are also allowable for at least the same reasons that their respective independent claims are allowable.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By 

Leslie A. Van Leeuwen, Reg. No. 42,196
Joseph T. Van Leeuwen, Reg. No. 44,383
Van Leeuwen & Van Leeuwen
Attorneys for Applicant
Telephone: (512) 301-6738
Facsimile: (512) 301-6742